



LARRY HOGAN
GOVERNOR

BOYD K. RUTHERFORD
LT. GOVERNOR

STATE OF MARYLAND
MARYLAND STATE POLICE
1201 REISTERSTOWN ROAD
PIKESVILLE, MARYLAND 21208-3899
410-486-3101
TOLL FREE: 1-800-525-5555
T D D: 410-486-0677



COLONEL
WILLIAM M. PALLOZZI
SUPERINTENDENT

July 9, 2019

MuckRock News
DEPT MR 75715
411A Highland Ave
Somerville, MA 02144-2516

Attn: Emma Best.

Re: PIA Requests

- 1) MOU's with ICE
- 2) Roll Call Release IA-0181-15

Dear Emma Best:

The Maryland State Police has received your requests (copies enclosed) under the Public Information Act (Annotated Code of Maryland, General Provisions Article §§4-101 through 4-601). We received your request on June 26 and June 27, 2019.

Upon receiving your request related to any/all MOU's between Maryland State Police (MSP) and Immigration, and Customs Enforcement (ICE), the enclosed MOU has been identified. The MOU, dated December 2011, addresses internet crimes against children. Please note that the enclosed document is the only MOU MSP has/had with ICE for the timeframe indicated.

As for your request related to a "Roll Call Release IA-0181-15", MSP has no records related to the release.

Having responded to your request, the Maryland State Police now considers this matter to be closed.

Sincerely,

Mark Urbanik
Interim Public Information Act Coordinator

"Maryland's Finest"





Mark Urbanik -State Police- <mark.urbanik1@maryland.gov>

PIA Log #19-1271

1 message

MSP PIA -State Police- <msp.pia@maryland.gov>
To: Mark Urbanik -State Police- <mark.urbanik1@maryland.gov>

Thu, Jun 27, 2019 at 4:10 PM

Hello this is a duplicate. Forwarding

Karen Waters
410 281-2702

----- Forwarded message -----

From: <75972-60741460@requests.muckrock.com>
Date: Mon, Jun 24, 2019 at 11:30 AM
Subject: Maryland Public Information Act Request: ICE MOUs/MOAs (Maryland State Police)
To: <msp.pia@maryland.gov>

Maryland State Police
PIA Office
1201 Reisterstown Road
Pikesville, MD 21208

June 24, 2019

To Whom It May Concern:

Pursuant to the Maryland Public Information Act, I hereby request the following records:

Copies of any Memoranda of Agreement (MOAs), Memoranda of Understanding (MOUs), memoranda of agreement or other liaison, information sharing or prisoner/detainee transfer agreements or delegations of authority with or involving Immigration and Customs Enforcement signed or otherwise put into effect between March 1, 2003 and the present. This includes but is not limited to any agreements entered into under or a result of Section 287(g) of the Immigration and Nationality Act.

I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the Internet Archive and MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As such, it is not necessary for me to demonstrate the relevance of this particular subject in advance.

As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

Sincerely,

Emma Best

Filed via MuckRock.com

E-mail (Preferred): 75715-36196668@requests.muckrock.com

Upload documents directly: https://accounts.muckrock.com/accounts/login/?url_auth_token=AAAY_a39UWgQOh2ZSRhVhhMQQi%3A1heN5j%3A1KH5zzpDrnfvPrsPGM7KNVsajvU&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fmaryland-state-police-834%252Fcriminal-hackers-target-police-to-protest-perceived-injustices-maryland-state-police-75715%252F%253Femail%253Dmsp.pia%252540maryland.gov

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News
DEPT MR 75715
411A Highland Ave
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.

--
Maryland State Police
Central Records Division
1711 Belmont Avenue
Baltimore, MD 21244
Phone 410 281-2716
Fax 410 281-2730

 **DHS-FBI-HackersTargetPolice.pdf**
259K



Mark Urbanik -State Police- <mark.urbanik1@maryland.gov>

PIA Log #19-1271

1 message

MSP PIA -State Police- <msp.pia@maryland.gov>
To: Mark Urbanik -State Police- <mark.urbanik1@maryland.gov>

Wed, Jun 26, 2019 at 3:42 PM

See Below

Karen Waters
410 281-2702

----- Forwarded message -----

From: <75715-36196668@requests.muckrock.com>
Date: Fri, Jun 21, 2019 at 1:12 PM
Subject: Maryland Public Information Act Request: Criminal Hackers Target Police to Protest Perceived Injustices (Maryland State Police)
To: <msp.pia@maryland.gov>

Maryland State Police
PIA Office
1201 Reisterstown Road
Pikesville, MD 21208

June 21, 2019

To Whom It May Concern:

Pursuant to the Maryland Public Information Act, I hereby request the following records:

Records mentioning, describing or generated as a result of the 8 May 2015 Roll Call Release IA-0181-15 (which was designed to be shared widely with law enforcement) from the Department of Homeland Security's Office of intelligence and Analysis (I&A) in conjunction with the Federal Bureau of Investigation, titled "Criminal Hackers Target Police to Protest Perceived Injustices," as well as records otherwise responding or reacting to the issues raised in it.

I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself.

As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

Sincerely,

Emma Best



ROLL CALL RELEASE

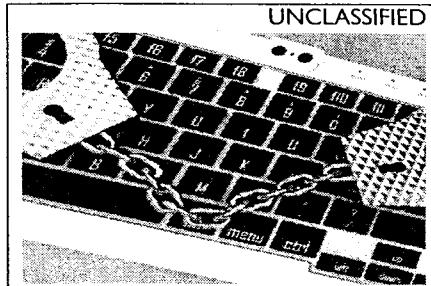
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.



(U) Figure 1. Criminal Hackers Targeting Police

(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

MARYLAND STATE POLICE
ROUTING SLIP

RE: MOU between MSP and US Immigration and Customs Enforcement (ICE) – Internet Crimes Against Children (ICAC) Task Force

TO: Legal Counsel Unit

DATE: December 15, 2011

FROM: *John Wilhelm*, L. John Wilhelm, Commander, Computer Crimes Section

COMMENT: Attached is an MOU between the MSP and the US Immigration and Customs Enforcement (ICE). This MOU formalizes a partnership between the two agencies related to investigating Internet crimes against children and prosecuting offenders.

Forwarded for legal review.

TO:

DATE:

FROM: Legally Sufficient

COMMENT: *Mark J. Baker*

Date 12/19/11
Legal Counsel Unit
Maryland State Police

TO:

DATE:

FROM:

COMMENT:

TO:

DATE:

FROM:

COMMENT:

DEC 16 2011

MEMORANDUM OF UNDERSTANDING

between the

MARYLAND STATE POLICE

and the

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
HOMELAND SECURITY INVESTIGATIONS
SPECIAL AGENT IN CHARGE, BALTIMORE

regarding the

MARYLAND INTERNET CRIMES AGAINST CHILDREN TASK FORCE

PURPOSE

The purpose of this Memorandum of Understanding (MOU) is to formalize working relationships between the Maryland State Police (MSP) and U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Special Agent in Charge (SAC), Baltimore, Maryland, to achieve maximum cooperation in a combined law enforcement effort aimed at combating Internet crimes against children in the State of Maryland and nationwide. Through this MOU, the participants agree to participate in the Maryland Internet Crimes Against Children Task Force (MDICAC) for the purpose of promoting a coordinated effort in investigating and prosecuting said crimes. Through participation in MDICAC, participants will benefit from grant resources, joint operations, and training opportunities. This MOU is not intended and should not be construed to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, the United States, the State of Maryland, or the officers, employees, agents, or other associated personnel thereof.

AUTHORITY

The authority for ICE to enter into this MOU is the Homeland Security Act of 2002, codified in Title 6, United States Code (U.S.C.).

MISSION

The MDICAC mission is to increase the effectiveness and efficiency of investigations and prosecutions of Internet crimes against children offenses, and to increase public awareness and prevention of these offenses. MDICAC's objectives are to: (1) increase the investigative capabilities of Maryland law enforcement officers in the detection, investigation, and apprehension of offenders; (2) conduct proactive and reactive ICAC investigations; (3) increase the number of ICAC offenses being prosecuted; (4) create a multi-agency task force response to ICAC offenses in the State of Maryland; (5) enhance the nationwide response to

ICAC offenses; and (6) develop and deliver ICAC public awareness and prevention programs.

POLICY AND DIRECTION

The MDICAC is the recipient of a federal grant disbursed by the U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, in Washington, D.C., and accordingly complies with the current version of the ICAC National Bylaws and Program Standards. The MDICAC Project Director, assigned to the Maryland State Police, Criminal Investigation Division, Computer Crimes Section, is responsible for the policy, coordination, and general direction of the MDICAC. The day-to-day operation and administrative control of MDICAC Task Force members will be the responsibility of the member agency's supervisory and administrative systems.

INVESTIGATIONS

All MDICAC investigations will be conducted in a spirit of cooperation, following ICAC Task Force National Program Standards, MDICAC guidelines, and each task force member agency's respective policy manual or guidelines. The principal sites of task force activity will be within the jurisdictional areas of the respective member law enforcement agencies, consistent with the level of membership of that law enforcement agency and statutes governing mutual aid. It is agreed that unilateral acts on the part of task force members involved in task force investigations are not in the best interest of the MDICAC Task Force.

CONFIDENTIAL INFORMATION

It is understood that any confidential information pertaining to investigations of Internet and technology crimes will be held in the strictest confidence, and will only be shared with participating MDICAC members or other law enforcement agencies where necessary with the approval of the agency that authored the record or produced the information or as otherwise required by federal law. Information provided by ICE to MSP shall not be released to non-law-enforcement entities. If this information is responsive to a request from a member of the public under Maryland Public Information Act, MSP agrees to coordinate such release with ICE.

EVIDENCE

Seized evidence and any other related forfeitures will be handled in a manner consistent with the policies of the task force member's agency.

PROCEDURES

A. INVESTIGATIVE RECORDS AND REPORTS

Each task force member will maintain their own agency records and reports. To the extent possible, all investigative information will be available to MDICAC members as it pertains

to investigations of Internet crimes against children, with the approval of the agency that authored the record or report.

B. PROSECUTION

When necessary, case-by-case analysis will be performed on each potential prosecution to determine in which jurisdiction the case will be prosecuted. A preference will be given to the jurisdiction that initiated the prosecution. Those cases being considered for federal prosecution will be investigated pursuant to the U.S. Attorney General Guidelines.

C. MEDIA RELATIONS

Media release information regarding MDICAC operations will be coordinated and made jointly by all participant agencies, and information pertaining to the Task Force will not be released to the media without the approval of participant agencies. Media releases shall not include information regarding specific investigative techniques or information that may compromise ongoing investigations.

D. LIABILITY

Each agency shall assume the responsibility and liability for the acts and omissions of its own officers, agents, or employees in connection with the performance of their official duties under this MOU. For tort liability purposes, no participating agency shall be considered the agent of the other participating agencies. Each participating agency shall be liable (if at all) only for the torts of its own officers, agents, or employees that occur within the scope of their official duties.

E. MODIFICATIONS TO AGREEMENT

This agreement may be modified upon the mutual written agreement of the parties. At the sole discretion of the MSP, additional agencies may join the MDICAC. New participating agencies will review the current MOU in force, and the agency's authorized representative will sign an addendum to the MOU signifying that they have read the MOU and agree to abide by terms. Current member agencies will then be notified of the addition of the new agency. Nothing in this MOU should be construed as limiting or impeding the basic spirit of cooperation that exists between the participating agencies.

F. DURATION

This MOU shall remain in effect until any agency elects to terminate the agreement. Continuation of this MOU shall be subject to the availability of necessary funding. This agreement may be modified at any time by written consent of all involved agencies. This agreement may be terminated at any time by any of the participating agencies, including the MSP. The participating agencies may withdraw from this agreement at any time by providing a 30-day written notice of its intent to withdraw to all other participating agencies. Upon withdrawal from or termination of the MDICAC and the MOU, all equipment purchased with federal MDICAC funds will be returned to the MSP.

G. POINTS OF CONTACT

ICE/HSI:

Veronica Ryan
Group Supervisor
Intellectual Property Rights/Child Exploitation Group
Homeland Security Investigations
U.S. Immigration and Customs Enforcement
40 South Gay Street
Baltimore, Maryland
Office Telephone: (410) 779-7496
E-mail Address: Veronica.Ryan@dhs.gov

Maryland State Police:

Lieutenant John Wilhelm
Commander
Computer Crimes Section
Maryland State Police
7155 Columbia Gateway Drive, Suite C
Columbia, Maryland 21046
Office Telephone Number: (410) 953-8260
Facsimile Number: (410) 290-1831
E-mail Address: Jwilhelm@mdsp.org

H. AUTHORIZATIONS

As witnesseth our hands on the dates shown.

ATTEST:

Date

MARYLAND STATE POLICE

By: Colonel Marcus Brown
Colonel Marcus Brown
Superintendent Maryland State Police

Approved for Form and Legal Sufficiency

ATTEST:

Date

By: Mark T. Brown 12/19/11
Legal Counsel Unit

ATTEST:

Date

(U.S. Immigration and Customs Enforcement)

By: WW 12/9/11

William Winter
Special Agent in Charge
Homeland Security Investigations

Approved for Form and Legal Sufficiency

ATTEST:

Date

By: _____
Legal Counsel Unit

*Homeland Security Investigations
Mission Support*

500 12th Street, SW
Washington, D.C. 20536



**Homeland
Security**

MEMORANDUM FOR: James A. Dinkins
Executive Associate Director

THROUGH: Peter T. Edge *Markel*
Deputy Associate Director

FROM: Staci A. Barreira *AS*
Assistant Director

SUBJECT: Memorandum of Understanding with the Maryland State Police
Regarding the Maryland Internet Crimes Against Children Task
Force

Issue:

This memorandum requests your review and approval of the enclosed draft Memorandum of Understanding (MOU) between the Maryland State Police (MSP) and the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agent in Charge (SAC) Baltimore, regarding the Maryland Internet Crimes Against Children Task Force (MDICAC).

Background:

The MDICAC's objectives are to increase the investigative capabilities of Maryland law enforcement officers in the detection, investigation, and apprehension of offenders; conduct proactive and reactive Internet Crimes Against Children (ICAC) investigations; increase the number of ICAC offenses being prosecuted; create a multi-agency task force response to ICAC offenses in the State of Maryland; enhance the nationwide response to ICAC offenses; and develop and deliver ICAC public awareness and prevention programs.

The signatories for this MOU will be William Winter, SAC Baltimore and Colonel Marcus Brown, Superintendent, MSP.

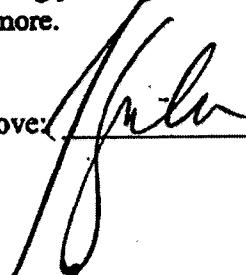
Memorandum of Understanding with the Maryland State Police Regarding the Maryland Internet Crimes Against Children Task Force

Page 2

Recommendation:

This MOU has been reviewed for legal sufficiency by the Office of the Principal Legal Advisor. I recommend approval of the enclosed MOU. If you approve, please indicate below by providing your signature and the date. The package will then be returned to the HSI SAC Baltimore.

Approve:

 Date: _____

Disapprove: _____

Date: _____